RFC 2350
UNISAYogya-CSIRT EN

UNIVERSITAS ‘AISYIYAH YOGYAKARTA

Kampus Terpadu:
Jl. Siliwangi (Ring Road Barat) No. 63 Mlangi, Nogotirto, Gamping, Sleman, Yogyakarta. 55292 Telepon: (0274) 4469199 Fax.: (0274) 4469204
Email: info@unisayogya.ac.id

RFC 2350

UNISA Yogyakarta *Cyber Security Incident Response Team*

UNIVERSITAS ‘AISYIYAH YOGYAKARTA

2022

arranged by:

UNISAYogya-CSIRT

Badan Pengembangan Teknologi dan Sistem Informasi

Kampus Terpadu:
Jl. Siliwangi (Ring Road Barat) No. 63 Mlangi, Nogotirto, Gamping, Sleman, Yogyakarta. 55292 Telepon: (0274) 4469199 Fax.: (0274) 4469204
Email: csirt@unisayogya.ac.id

1 Information regarding this Document

The document contains UNISAYogya-CSIRT description based on RFC 2350, it provides basic information regarding UNISAYogya-CSIRT, its explaining responsibility, services, and how to contact UNISAYogya-CSIRT.

1.1 The Latest Update

The current version is 1.0 and published on 19 September 2022.

1.2 Distribution Lists for Notifications

There is no distribution lists for notifications.

1.3 The Location Of this Document

The current version of this document can always be found at:
https://csirt.unisayogya.ac.id/rfc2350-en.pdf

1.4 Authenticating this Document

This document has been signed with the SSL of UNISAYogya-CSIRT. See section 2.8 for details.

1.5 Document Identification

The document's attributes :

Title	: RFC 2350 UNISAYogya-CSIRT EN;
Version	: 1.0;
Publish	: 19 September 2022;
Expiration	: This document is valid until superseded by a later version

2 Data Information / Contact

2.1 Team

Universitas Aisyiyah Yogyakarta-Cyber Security Incident Response Team
Short Name : UNISAYogya-CSIRT.

2.2 Address

Jl. Siliwangi (Ring Road Barat) No. 63 Mlangi, Nogotirto, Gamping, Sleman, Yogyakarta. 55292

2.3 Time Zone

Yogyakarta (GMT+07:00)

2.4 Phone

+62 895-2940-5592
(24/7)

2.5 Fax

(+62274) 4469204

2.6 Other Communications

-

2.7 E-mail

csirt@unisayogya.ac.id

2.8 Public Key and Encryption Information

2.8.1 Provision

a SSL used to sign digital signature, if fails use PGP

b PGP used to encrypt email messages

2.8.2 Public keys

- ☐ Public keys installer and downloader on Windows
  https://csirt.unisayogya.ac.id/RootUNISAYogyaInstaller.bat
- ☐ How to sign and validate digital signature
  https://csirt.unisayogya.ac.id/CaraValidasiDigitalSignature
- ☐ Encrypted messaging guide
  https://csirt.unisayogya.ac.id/EmailDenganPGP

a PGP

-----BEGIN PGP PUBLIC KEY BLOCK-----

xsDNBGMa3soBDAC/h6B4FD3AR50a6/ALbLqd10tXLWd9SQ2XkTe4kuDGjL+MUJoc
9ERcr2dNZ9UVjeSIjUVZwdGfawxuhMpFlfQF5Z27jVSrNfWJv4Q4lFShYY8CQ+w4
XGh44B3qygFdUxEwwD86DcBBAqQyN9vqpkF3ynu/X0vyle36tqwXZVZinNM5UtuU
mB8U7wHmc8ijbZtMqaxUi8RHu1lKdcSTyrGYpPbrOWvDA/YCaGLx6jjZFcMjc+tG
xWezMW1RbwwyeHtjWqJMRvx2Tgygjh9RiijAV30/SNtU69go3zebGryqpFyB6Mwu
r5nRrBBiij7d3ALvcHo1og0RjH8Wve9VY71eJp83YhV28+5yXHUuLWJCrJAZK2H7
yrPEYTJSnpJP7X4TYutqcjfiFqd9nvOF+EWZgeudUhwSgwT9vQJnNG88PgNr2IJR
YdOiQbIa7Gos5rS16UmXpODoeaRHYh0kHuqhsMQ4/5arsSOcw9wEhuJ3sQebhwKY
hbaCJmDr4h8+gUkAEQEAAc0pVU5JU0FZb2d5YS1DU0lSVCA8Y3NpcnRAdW5pc2F5
b2d5YS5hYy5pZD7CwQ0EEwEIADcWIQQD0sLfkwCWDtAm6v5S7Ka8jwaikQUCYxre
zAUJEswDAAIbAwQLCQgHBRUICQoLBRYCAwEAAAoJEFLspryPBqKRh30L/REfR1OE
UGjobr2zBcxl2qUOGULKI5fukShSp8RvTiJpStCq+6MwglOTNkeU17JK3PFUZSVS
5gydMOJoTNkFhRU7o19cIU9kYWWixgrS/tFHe8o1cDc2xaaO6X768XbQpiR0lY+T
QXWdpuVB7+279JXgq+ODpqjCRYZ8j+4a2nTj5po54AtGA5CPLdnpt4c7+8NHNybq
dlYtwvc+rk78zbBocknKQhygoMFMAgvWdbSde8FDaL1xJ0A6JcFys5/Q96x7Zw8g
9YdwqqHMZkE6XWnmxRxzeIL6KqCUU2zaNihy8vGJMqm3dicQITvUapTZmRHwis4Z
ldXFey2VNaYOuXwkt/3G/QfjrotPrYVX+Bx2jWRRHntUwaUetENFlrh6/0TSFgVY
G4wdLCaqLQRnqyrbv8ciWADSGzq3DR3Y3mI7W/eK1NdCLUt/S10/o8SjdEdPmcVU
xJmsMJUJqehzcHZPJ0AeJy2BzfZd6PHwUvsmXX0XMWKRhY+pjryB7fVZp87AzQRj
Gt7MAQwAqBHpX4nGWKt5hvsx/2RexQ7kNfIkVM+R7PXYqwsWtWAywuvPcLUWnmcY
Lw2/oT2XBgdcEovYYbR1Ckxz1wLj6bpup1C72UyyRO8ZOL6whYU83WyRVl8NELka
jV54SPolTZJ7UPI7JYBCt8omp6KaHiIED/qGjU2wie3BsgptFAUY3aXQurFpn8Ms
amRrfeCqjmZI7KMS4ohIIydsZgOWo6SJeudHYnhK6DXfqTupRZN5Ycr6kVCVbqkO
HpWF6SpDJyguclOakVb04mb9cK02N5kIRxv2D3O6B46Ws6vTk1JUZ0Kyrcles+d0
tOXEjvNfs4UwHkgUcFr58g//dNfUgMxzPgmOG3MKrJebZo3nvhBVqwdi0nDH7Gxr

CC+Tpase0N13/KWbkgxZVflTkSkh3NFbzEFfNq9ZFsyXo6qhFMPOQwXa9xj8CY8H
VgKFccXY1tp8Mou9agy5jQltW57las3klsHXk21nw4v8fh/85S1UKcu5AQR9MMsY
SQPrmJuRABEBAAHCwPwEGAEIACYWIQQD0sLfkwCWDtAm6v5S7Ka8jwaikQUCYxre
1AUJEswDAAIbDAAKCRBS7Ka8jwaikaQ7C/9S1SAb0PDaL9t8tfh2CIqSrg8omBfO
byxglm2cXAym8pkfWTgWTLUJuBdHlhzCTRHpU3l5aFaBrLxY4A/0UapDbKuipIca
qgVu44xkQwB4/ejbUEjuaVKyTLyLY5OFK/F0gVhcQVMkqGzDcQlInaxO/bJ/x5KX
NOBguDKrY18c3RkPsunbt9TeY5fLd9CivkmrcVma/wrWy8ImsxkU/KibBziElGGn
Bltj3aEXjskk6i0YVMnaOwueOsAo1ZsS0NXUQLJCmfyHbkI4gTtXC/8a74YXNmNr
4wvw6l2paFIIv9BhARfjC3z0lgG1IT8LP+6bRbqA6YB5XoxBldh9LrSScJURf/4E
jyHctZpGFWqpiRo6onkUytRk5IDLFiy56+ORjuyrX7+QHr+47gRHnv6Gw6N/b6AW
NswTJpACE61wIM3NUtcc+6ljMb9i/fPWhjRBp4xHGEQK3o6uB2gc0yZFNx4foQME
EEPnLsR0K8fS4EKefTZMRRvVKCqNpBGh3DQ=
=6PgP

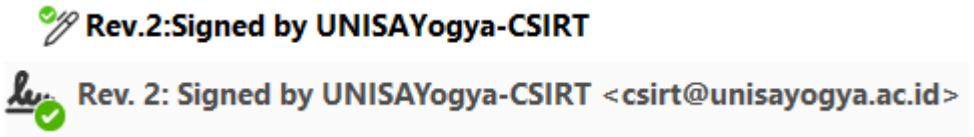
-----END PGP PUBLIC KEY BLOCK-----

Finger Print : 03D2 C2DF 9300 960E D026 EAFE 52EC A6BC 8F06 A291

PGP key availability :

- ☐ Public key
  https://csirt.unisayogya.ac.id/UNISAYogya.asc

b SSL for Digital Signature



-----BEGIN CERTIFICATE-----
MIIGQzCCBCugAwIBAgIJAPXvR2ipR+xnMA0GCSqGSIb3DQEBCwUAMIG2MQswCQYD
VQQGEwJJRDETMBEGA1UECAwKWW9neWFrYXJ0YTETMBEGA1UEBwwKWW9neWFrY
XJ0
YTEpMCcGA1UECgwgVW5pdmVyc2l0YXMgJ0Fpc3lpeWFoIFlvZ3lha2FydGExGTAX
BgNVBAsMEFVOSVNBIFlvZ3lha2FydGExETAPBgNVBAMMCFVOSVNBIFlrMSQwIgYJ
KoZIhvcNAQkBFhVpbmZvQHVuaXNheW9neWEuYWMuaWQwIBcNMjEwOTI3MTY1NDUw
WhgPMjA3MTA5MTUxNjU0NTBaMIG2MQswCQYDVQQGEwJJRDETMBEGA1UECAwKWW
9n
eWFrYXJ0YTETMBEGA1UEBwwKWW9neWFrYXJ0YTEpMCcGA1UECgwgVW5pdmVyc2l0
YXMgJ0Fpc3lpeWFoIFlvZ3lha2FydGExGTAXBgNVBAsMEFVOSVNBIFlvZ3lha2Fy
dGExETAPBgNVBAMMCFVOSVNBIFlrMSQwIgYJKoZIhvcNAQkBFhVpbmZvQHVuaXNh
eW9neWEuYWMuaWQwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCsKyLz
Hf2lOysNPeIvKxIsOCE1/5Fs3zPfce4BWjKsFkKdgtcorTav+PqbRzzqHxcsWoBE
ObkaYQBYETo+t6jKJKHfVtSlvQuvhuqjNOKboiPfxje0OVbVsLRgq0KPwci8/dBi
ros77F7bQu3kUThBhjfWJhulGwmYgjTFeUbdosh1INDelUWKNL4m1WErxvDjno8M
tWSeNZFCg8/9PC3Ic0rGwQhVbXprlAslkJmc821ith4KWNrW30sxOd8aOLmCuOFS
Ix1jFXF3HO4VWgGI6jjvR1aImXmjGJ3LuZiRj/sVy4QbrwHsuMbfL2Q/Jo1IFVaq
jfioovjrPi7o9brQ/IbytpCoxvJNYUgzcVv0K6BKYp+MeO7gmH1kLHpSWIyEn0vW
XNmIVuxLKI+PdW8AdkmWgXbAtzIEbWZ5CvpAAdrcTQ5ZSAR/vlYJu3IFQwuwF3N5
7bkomPRaW/YO5V9BbQ6wKcCoeOUMGXDYYb35VZlpW2XSDam9dTYa+5nv5Jo00zgA
ckewSDnuxbUyDrKAjZSye7BJCRYLMsljHQM/ZgmyAkrxE1+c3SyCUsnWh7Pm5nw8

+VcEhiv2NsHad+XQyjuFOS/3+5y+ah5094GWE9xyaLERujICnFOC9/tDrPQjAMwY
7u22+s4WdJliE4h57Wvpqwan3bY7URo3w0SSpwIDAQABo1AwTjAdBgNVHQ4EFgQU
BKNQX3INzLPr9hOpfJchbUwhd2MwHwYDVR0jBBgwFoAUBKNQX3INzLPr9hOpfJch
bUwhd2MwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAJtl3IRYZtzw0
+ec9ivX+ur9JrLiTdCx7sJD3rfCfdfH5IVXaOEIIFu5wfBnxB16MwL6QE8b19Ok6
zBUrJr9FWKYiCYAJI/iCj8Wx8iHJtkd1vYaqefYHoMZ31ICAYH+r0SMRqbVpylGW
u6XLXysyimW51z5F3n1mBek9YIlvPQxti9fdO/eedkd4QlsQnsaKsd8IasihWBtB
rkcOnGUTL+ac6h2LVQgkex7Ex9EZZX2Dn9v7GrhobwNku3iD00E5o/HqdjavBVPk
cNS9V3NEXhm8By+Ho7EGM+84TNncqXKVJCKo0DZGr+FnR0fAUzHc96RlQIGwqV+w
n7r9M4wQVVpM/rDvFvUaoYoHUznxBZd9bNd0VuMyjzjMl7tYp4m7tMKakDnbnmwm
JZWbWl8zdB8yA0psjPKDgs37zHOQOaduqCWLJn0jRLTCowsdFtcJ2DLK+e+ajeMk
H54qpZ/BmSn3LtnOvwFkWEWIgfbb2NyTiN2ZHXQftanrOvJWyaRbqHtGXFtAvDpB
PtkCBsutG35s9RCoYeb0PHLBsvKUg/VABdECCqmCBRB/IYw8GU+kzVJkCCO3oCRS
5tixTQoViFquY1IGdUcR11SOiWvqcTvLdM1i6KJ6E9hV1wqvj5nnWNMSBgsvxYNJ
YF1WXvgTpUCnTwuvvjGs86KgGlinXCc=
-----END CERTIFICATE-----

SSL's Certificate Authority availability:

- ☐ Certificate Authority
  https://csirt.unisayogya.ac.id/rootCAUNISAYogya.cer
- ☐ Revocation List
  https://csirt.unisayogya.ac.id/rootCAUNISAYogya.crl.pem
- ☐ Adobe Reader FDF
  https://csirt.unisayogya.ac.id/CertExchangeUNISAYogyakarta.fdf

2.9 Members

2.9.1 Team

a Head (Coordinator of PTSI Eksternal dan Jaringan)
Ikhwan Hawariyanta, S.T.

b Members
Arizona Firdonsyah, S.Kom., M.Kom.
Nurul Latifah, S.Kom.

2.9.2 Contact

Nurul Latifah, S.Kom.

2.10 Other Information

-

2.11 Points of UNISAYogya-CSIRT Contact

The preferred method to contact UNISAYogya-CSIRT is by e-mail at csirt@unisayogya.ac.id or by phone +62 895-2940-5592 on weekdays at 08.00 – 15.00 +7 GMT or on call 24/7.

3 About UNISAYogya-CSIRT

3.1 Vision

Cyber security realization in Universitas Aisyiyah Yogyakarta's information and communication technology management

3.2 Mission

a Developing, coordinating, collaborating and operating the preventions, activities and rehabilitations of cyber incident within Universitas Aisyiyah Yogyakarta;
b Developing cooperation in cyber security of IT services within Universitas Aisyiyah Yogyakarta.
c Increase human resources capacity against cyber threat on cyber security incident's prevention, activity and rehabilitation aspects within Universitas Aisyiyah Yogyakarta.

3.3 Constituent

Unisayogya-CSIRT constituents are users of IT services within Universitas Aisyiyah Yogyakarta.

3.4 Sponsorship and/or Affiliation

UNISAYogya-CSIRT funding source is from Universitas Aisyiyah Yogyakarta.

3.5 Authority

UNISAYogya-CSIRT authorized to handle, mitigate, investigate and analyze cyber security threat within Universitas Aisyiyah Yogyakarta with constituent. UNISAYogya-CSIRT can coordinate or collaborate with other competent unit for unhandle incident, such as BSSN and/or IT security and/or other security experts.

4 The Policies

4.1 Types of Incidents and Support Level

UNISAYogya-CSIRT handle various cyber security incident as follow :

a Web Defacement;
b DDoS;
c Malware;
d Ransomware;
e Phising;
f SQL Injection;
g Social Media Account Hijacking;
h Illegal Access;
i Spam.

Support given by UNISAYogya-CSIRT to the constituent depends on incident type and impact. Incident handling services based on constituent's report.

4.2 Collaborations, Interactions and Disclosure of Information/Data

UNISAYogya-CSIRT will collaborate and share information with other CSIRT or organization in cyber security scope. All information received by UNISAYogya-CSIRT will be confidential.

4.3 Communications and Authentication

UNISAYogya-CSIRT can use unencrypted message and telephone for regular communications. All sensitive/limited/secret material will PGP encrypted.

5 Services

5.1 Main Services

Main services of UNISAYogya-CSIRT :

5.1.1 Cyber Security Warning

This service coverage are cyber security incident warning to owner electronics system and statistical information managed by each unit within Universitas Aisyiyah Yogyakarta.

5.1.2 Cyber Security Incident Handling

This service coverage are coordination, analysis, technical recommendation and on-site assistance in cyber security incident handling within Universitas Aisyiyah Yogyakarta.

5.2 Additional Services

Additional services of UNISAYogya-CSIRT :

5.2.1 Electronic System Vulnerabilities Handling

This service coverage are software and hardware vulnerabilities checking, and do a vulnerabilities verification for possibilities of exploit with the aim to developing plan to recovery identified vulnerabilities. Terms of this service:

a Reporter is electronic system owner. If reporter is not the owner, then report is ignored;

b This can be vulnerability assessment and stress test follow up.

5.2.2 Digital Artifact Handling

This service coverage are artifacts handling in the term of electronic system recovery or investigation support by providing services statistical information within Universitas Aisyiyah Yogyakarta. This activity is in the form of technical analysis carried out to find digital traces in the form of objects or documents that are allegedly used to commit acts against the law against Electronic Systems.

5.2.3 Potential Threats Observation Notice

This service coverage is delivering information to constituents regarding threats to electronic systems that can arise due to the influence of technological, political, economic and other developments.

5.2.4 Attack Detection

This service coverage is data analysis activities in order to detect attacks on Electronic Systems.

5.2.5 **Cyber Security Risk Analysis**

This service coverage is cyber security risk assessment process, including: identification, analysis, and evaluation of risks, as well as determining control options for the risks. Risk control techniques consist of avoiding, transferring, mitigating, and accepting risks.

5.2.6 Incident Handling Readiness Consultation

This service coverage is counseling activities carried out with the aim of providing insight, understanding, and ways that need to be carried out in order to assist in handling cyber incident.

5.2.7 **Building Cyber Security Awareness And Concern**

This service coverage is dissemination in the field of cyber security to constituents which aims to provide an understanding of the dangers contained in cyberspace and how to overcome them.

6 Incident Reporting

Cyber security incident reports sent to csirt@unisayogya.ac.id by attaching at least :

a ID Card photo/scan
b Photos or screenshots or log files of incident as evidence
c Reporter phone number
d Or satisfy other applicable provisions

7 Disclaimer

Cyber security incident handling depends on tools available.

CSIRTUNISAYogya

2022.09.19 13:56:33+07'00'